

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DAVID MUTNICK, for himself and others)
similarly situated,)
Plaintiff,) Case No. _____
v.)
CLEARVIEW AI, INC., HOAN TON-THAT and) CLASS ACTION COMPLAINT
RICHARD SCHWARTZ,) JURY TRIAL DEMANDED
Defendants.) INJUNCTIVE RELIEF DEMANDED
)
()

CLASS ACTION COMPLAINT

Plaintiff DAVID MUTNICK, on behalf of himself and all other similarly situated individuals (“Plaintiff”), by and through his attorneys, brings this Class Action Complaint against Defendants CLEARVIEW AI, INC., HOAN TON-THAT and RICHARD SCHWARTZ and alleges the following:

INTRODUCTION

1. Almost a century ago, Justice Brandeis recognized that the “greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.”¹ The conduct of Defendant Clearview, as alleged herein, epitomizes the insidious encroachment on an individual’s liberty that Justice Brandeis warned about. However, unlike the “men of zeal” described by Justice Brandeis, Defendant Clearview’s conduct was not well-meaning. Rather, Defendant Clearview acted out of pure greed.

¹ *Olmstead v. United States*, 277 U.S. 438, 479 (Brandeis, J., dissenting).

2. Without obtaining any consent and without notice, Defendant Clearview used the internet to covertly gather information on millions of American citizens, collecting approximately three billion pictures of them, without any reason to suspect any of them of having done anything wrong, ever. After obtaining these images, Clearview used artificial intelligence algorithms to scan the facial geometry of each individual depicted in the images, a technique that violates multiple privacy laws. Clearview now furnishes this data to law enforcement agencies throughout the United States, including law enforcement agencies in Illinois, for a fee. Much like dossiers that police departments keep on prior suspects and convicted criminals to use in future investigations, these agencies are now using Clearview's database. However, almost none of the citizens in the database has ever been arrested, much less been convicted. Yet these criminal investigatory records are being maintained on them, and provide government almost instantaneous access to almost every aspect of their digital lives.

3. What Defendant Clearview's technology really offers then is a massive surveillance state with files on almost every citizen, despite the presumption of innocence. Indeed, one of Defendant Clearview's financial backers has conceded that Clearview may be laying the groundwork for a "dystopian future." Anyone utilizing the technology could determine the identities of people as they walked down the street, attended a political rally or enjoyed time in public with their families.

4. Moreover, by controlling the database privately, Clearview received, and continues to receive, real-time access to criminal investigations – it knows who the police are interested in and, often, where those people may be. Thus, Clearview is enmeshed in the use of state power against individual American citizens and, further, has the unique opportunity to tip-off and/or extort suspects.

5. Defendant Clearview's technology poses a grave threat to civil liberties. Constitutional limits on the ability of the police to demand identification without reasonable suspicion, for instance, mean little if officers can determine with certainty a person's identity, social connections, and all sorts of other personal details based on the visibility of his face alone.

6. Moreover, while Defendant Clearview developed its technology in conjunction with law enforcement, the technology is not inherently limited to that use. Clearview has gone on to provide its database to private entities including banks and retail loss prevention specialists. Further, Clearview has actively explored utilizing its technology to allow a white supremacist to conduct "extreme opposition research" and has developed ways to implant its technology in wearable glasses that private individuals could use.

7. Defendant Clearview did not develop its technology out of a desire for a safer society. Rather, Clearview developed its technology to invade the privacy of the American public and monetize citizens' rights for its own profit. In fact, Clearview created its database by violating each person's privacy rights, oftentimes stealing their pictures from websites in a process called "scraping," which violate many platforms' and sites' terms of service, and in other ways contrary to the sites' rules and contractual requirements. Thus, while trying to paint itself as a tool of law enforcement, Clearview actually has conspired with law enforcement to break the law, and violated citizens' rights under the U.S. Constitution in multiple ways, including violating the First Amendment, Fourth Amendment, Fourteenth Amendment and the Contracts Clause of Article I, among others.

8. Plaintiff brings claims on behalf of all American citizens in the Clearview database for injunctive relief to enforce these vital constitutional rights and for damages against

those responsible for this unconstitutional and anti-democratic scheme (the “Constitutional Rights Class”).

9. Plaintiff also brings claims on behalf of the citizens of Illinois in the database (the “Illinois Class”). Specifically, Defendant Clearview’s business model blatantly violates the privacy protections in the Illinois Biometric Information Privacy Act, 740 ILCS 13/1, *et seq.* (“BIPA”). In so doing, Defendant Clearview and the individually-named defendants unjustly enriched themselves at the expense of millions of unsuspecting individuals, including Illinois residents.

10. Defendant Clearview’s practices have injured Plaintiff and class members (“Class Members”) by, among other things, unlawfully obtaining their biometric identifiers and information without consent and, subsequently, selling or otherwise profiting from it.

11. Plaintiff and the Illinois Class retain a significant interest in ensuring that their biometric identifiers and information, which remain in Defendant Clearview’s possession, are protected from hacks and further unlawful sales and use. Plaintiff therefore seeks to remedy the harms Clearview and the individually-named defendants have already caused, to prevent further damage, and to eliminate the risks to citizens in Illinois and throughout the United States created by Clearview’s business misuse of millions of citizen’s biometric identifiers and information.

PARTIES

12. Plaintiff DAVID MUTNICK is an Illinois resident residing in the Northern District of Illinois. At relevant times, images of Plaintiff’s face appeared on numerous internet-based platforms and websites.

13. Defendant CLEARVIEW AI, INC. is a private, for-profit Delaware corporation, headquartered in New York, New York (Defendant and its predecessors, hereinafter

“Clearview”). Clearview markets its technology throughout the United States, including in Illinois. Moreover, Clearview obtains the images that underlie its technology from millions of internet-based platforms and websites, including, on information and belief based on the magnitude of platforms and websites involved, platforms and websites of Illinois companies or companies who operate servers in Illinois.

14. Defendant HOAN TON-THOT is a founder of Defendant CLEARVIEW AI, INC. and an architect of its illegal scheme, as alleged herein. RICHARD SCHWARTZ is a principal of CLEARVIEW and an architect of its illegal scheme. These defendants (collectively the “Individual Defendants”) are co-conspirators.

JURISDICTION AND VENUE

15. This Court has jurisdiction under 28 U.S.C. § 1331, as this case brings federal constitutional claims pursuant to 42 U.S.C. § 1983. It also has jurisdiction under 28 U.S.C. § 1332(d)(2) (the “Class Action Fairness Act”) because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and there are 100 or more members of the Classes. This Court has supplemental jurisdiction over all the state law claims pursuant to 28 U.S.C. § 1337.

16. This Court has personal jurisdiction over Defendant Clearview because Illinois citizens’ rights were a target of its conspiracy, it knew that its conspiracy would cause injury here, it markets and contracts to provide its database in Illinois, and it collected and sold the biometric identifiers and information of Illinois citizens in violation of BIPA. Moreover, without authorization, Clearview scraped images of Plaintiff and Class Members that Plaintiff and Class Members created in Illinois, uploaded from Illinois, and managed via their Illinois-based computers and mobile devices. Further, Clearview obtained the images of Plaintiffs and Class

Members from millions of websites, including Facebook, YouTube and Venmo. On information and belief, based on the magnitude of websites involved, some of the platforms and websites from which Clearview obtained its more than three billion images were operated by Illinois companies or companies with servers located in Illinois.

17. This Court has personal jurisdiction over the Individual Defendants because they conspired to further the illegal scheme alleged in this Complaint, knowing that it would take place, at least in part, in this jurisdiction and that it would injure citizens living here. The Individual Defendants knew or had reason to know that the scheme they devised would deprive Illinois citizens of their statutorily-protected privacy rights, neutralize Illinois citizens' ability to control access to their biometric identifiers and information via their Illinois-managed computers and social media accounts, and expose Illinois citizens to ongoing surveillance as they went about their lives within the state. Illinois citizens were subject to surveillance by any user of Clearview's services, including but not limited to the Springfield, Illinois Police Department and other Illinois governmental entities and businesses that had access to the database.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1331(b)(2) because a substantial part of the acts or omissions giving rise to the claim occurred in Illinois. Defendants obtained images uploaded from Illinois, violating the user agreements and terms of services of the websites to which they were uploaded. Moreover, had Defendant Clearview complied with BIPA, Class Members residing in this District and managing their social media accounts primarily from within the District would have been able to decide whether, for what purposes, and to whom they wanted to provide access to their biometric data. Clearview's failure to comply with BIPA—a principal omission giving rise to liability—is directed at this District.

Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Clearview.

ILLINOIS BIOMETRIC PRIVACY LAWS

19. According to BIPA, “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” 740 ILCS § 14/5(c).

20. BIPA seeks to safeguard individuals’ biometric identifiers and information.

21. Biometric identifiers include a scan of an individual’s face geometry. 740 ILCS § 14/10.

22. Biometric information is “any information . . . based on an individual’s biometric identifier used to identify an individual.” 740 ILCS § 14/10.

23. Pursuant to BIPA, a private entity, such as Defendant Clearview, is: (a) prohibited from collecting or otherwise obtaining an individual’s biometric identifiers and information without providing written notice and obtaining a written release; (b) prohibited from selling, leasing, trading or otherwise profiting from an individual’s biometric identifiers and information; (c) prohibited from disclosing, redisclosing or otherwise disseminating an individual’s biometric identifier or information unless specifically allowed by the statute; and (d) required to develop a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying biometric identifiers and information. 740 ILCS § 14/15.

24. BIPA provides for a private right of action and allows a prevailing party to recover liquidated damages in the amount of: (a) \$1,000 or actual damages, whichever is greater,

for negligent violations of its provisions; and (b) \$5,000 or actual damages, whichever is greater, for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also allows for the recovery of attorneys' fees and costs and injunctive relief. 740 ILCS § 14/20.

ALLEGATIONS

I. Allegations Related to Plaintiff

25. Plaintiff has been an Illinois resident, residing in the Northern District of Illinois since at least 2016.

26. At relevant times, Plaintiff posted photos of himself on various publicly-accessible platforms and websites. Plaintiff posted the photos described in the preceding sentence while located in the Northern District of Illinois.

27. At relevant times, others posted photos of Plaintiff on various publicly-accessible platforms and websites.

28. At relevant times, photos of Plaintiff have appeared on various publicly-accessible websites.

29. At no time did Defendant Clearview inform Plaintiff or a legally authorized representative of Plaintiff in writing that it had collected Plaintiff's biometric identifier or biometric information.

30. At no time did Defendant Clearview inform Plaintiff or a legally authorized representative of Plaintiff in writing of the specific purpose and length of term for which Plaintiff's biometric identifier and/or biometric information was being collected, stored and used.

31. At no time did Plaintiff or his legally authorized representative provide Defendant Clearview with an executed written release allowing Clearview to use his biometric identifier and/or biometric information.

32. At no time did Plaintiff or his legally authorized representative consent to Defendant Clearview disclosing or rediscovering his biometric identifiers and/or biometric information.

33. At no time did Plaintiff or his legally authorized representative consent to Defendant Clearview engaging in a process called “scraping,” whereby Clearview used an automated process to steal and convert to its own use online photos of Plaintiff and corresponding information associated with those photos. Indeed, in many instances, the terms of service of the platforms or websites on which Plaintiff’s photos were posted prohibited scraping. Where such prohibitions were in place, Clearview breached the contractual terms governing its use of the relevant websites and thereby harmed Plaintiff, a third-party beneficiary of those contracts.

II. Defendant Clearview’s Illegal Database

34. Based on publicly-available information, Defendant Clearview collected and obtained biometric identifiers and information from approximately three billion images – including, on information and belief, the biometric identifiers and information of Plaintiff and Class Members – and subsequently sold, traded, leased and otherwise profited from those biometric identifiers and information. Where Clearview acquired these images in violation of the contractual terms governing its use of the websites from which the images originated, Clearview impaired the rights of Plaintiff and Class Members, who were contractual parties and/or third-party beneficiaries of those contracts.

35. Defendant Clearview, by and through its principals Defendants Ton-That and Schwartz, carried out the surveillance scheme, at least in part, with members of law enforcement

that would allow Clearview to assemble the database as an agent of law enforcement using illicit techniques that the government on its own could not or would not use.

36. Based on publicly-available information, Defendant Clearview, by and through its principals Defendants Ton-That and Schwartz, has executed agreements with hundreds of state actors in jurisdictions throughout the country to deprive citizens of rights in a manner that the government agencies were prohibited from doing, would not do, or could not do, thereby: (a) making the public's biometric identifiers and information instantly available to law enforcement and other clients without any privacy safeguards, warrants or showing of reasonableness; (b) adding to the searchable database new photos uploaded by law enforcement clients; (c) making law-enforcement investigative activity visible in real time to Clearview's principals and employees; and (d) making available to law enforcement yet further identifying information about Plaintiff and Class Members, including social media profiles and online activity, uncovered by scanning and matching the biometrics in photos to those already in the database.

37. To date, Defendant Clearview has entered into service agreements with over 600 law enforcement agencies to the ends of creating, improving, updating and selling, leasing or otherwise profiting from its database. One such jurisdiction is the Springfield, Illinois Police Department.

38. Defendant Clearview provided customers, including law enforcement agencies, with a service agreement that ensured customers would have unlimited access to its database. The agreement made no mention of privacy protections, constitutional safeguards or limitations on information sharing of any kind.

39. In practice, those with access to Defendant Clearview's database could use the database to identify individuals via biometric searches and then share the results with other

interested entities, including law enforcement and private entities. As a result, a single user's biometric search could potentially snowball into a nationwide dragnet.

40. In violation of BIPA, Defendants collected, captured and otherwise obtained individuals' biometric identifiers and information – including, on information and belief, the biometric identifiers and information of Plaintiff and Class Members – without providing the requisite written information and without obtaining the requisite written releases.

41. In violation of BIPA, Defendants sold, leased, traded and otherwise profited from individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Members.

42. In violation of BIPA, Defendants disclosed, redisclosed and otherwise disseminated individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Members, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure or redisclosure; (b) the disclosure or redisclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure or redisclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

43. In violation of BIPA, Defendants did not develop a written policy that they made available to the public that established a retention schedule and guidelines for permanently destroying biometric identifiers and information.

44. Rather than complying with BIPA's notification and release requirements, Defendants did precisely the opposite, concealing their unlawful activities from Plaintiff and Class Members.

45. As a result of Defendants' violation of BIPA, Plaintiff and Class Members already have been injured and will continue to be injured, as set forth in more detail below.

III. Individual Defendants' Involvement in Clearview's Illegal Scheme

46. Pursuant to an understanding with the members of law enforcement, Defendant Clearview's principals – Defendants Ton-That and Schwartz – agreed to direct, directed and continue to direct, Clearview's employees to undertake the unauthorized scraping of photographic and other information from websites and to unlawfully extract biometric identifiers from billions of online images.

47. Defendant Schwartz paid for the servers and other costs necessary to carry out the scraping and scanning operations. This unlawful collection and storage of biometric data continues to this day. As of October 2019, Clearview boasted in an advertising email that "our database is also rapidly expanding 24/7. Every day, we add 40-50 million new images for you to search with Clearview."

IV. Plaintiff's and Class Members Injuries and Damages

48. As a result of Defendants' unlawful conduct, as alleged herein, Plaintiff and Class Members have suffered and will continue to suffer severe consequences. Defendants' conduct has resulted in, among other things: (a) Plaintiff's and Class Members' loss of constitutional rights to privacy and to prevent maintenance of personalized investigatory records without a prior conviction or just cause; (b) Plaintiff's and Class Members' loss of contractual rights; (c) unalterable biometric identifiers and information being collected and sold without their

permission; and (d) Plaintiff and Class Members being deprived of the very control over their biometric identifiers and information that BIPA was designed to protect. As a result of Defendants' misconduct, Plaintiff and Class Members have no recourse for the fact that their biologically unique information has been compromised. Moreover, Plaintiff and Class Members are at heightened risk for identity theft, stalking, and other potential injuries, are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action on behalf of himself as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiff seeks certification:

All American Citizens whose images are possessed by Defendant Clearview and for whom Clearview has scanned the facial geometry from those images (the "Constitutional Rights Class").

Persons in the Constitutional Rights Class include those for whom Defendant Clearview obtained images in violation of the terms of service or other contractual requirements of the websites on which the images were posted, as well those whose images were otherwise illegally obtained. Plaintiff also brings claims on behalf of himself as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following additional Class for which Plaintiff seeks certification

All persons residing in Illinois whose facial geometry was scanned by Defendant Clearview and subsequently sold, leased, traded, disclosed, redisclosed or otherwise used by Clearview to profit without Clearview having complied with BIPA's requirements (the "Illinois Class").

50. Excluded from the Classes are: (a) Defendant Clearview; (b) any parent, affiliate or subsidiary of Defendant Clearview; (c) any entity in which Defendant Clearview has a

controlling interest; (d) any of Defendant Clearview's officers or directors; or (e) any successor or assign of Defendant Clearview. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

51. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

52. **Numerosity.** Consistent with Rule 23(a)(1), the proposed Classes are so numerous that joinder of all members is impracticable. While Plaintiff does not know the exact number of members of the proposed Classes, Plaintiff believes the proposed Classes contain millions of people. Class Members may be identified through objective means, including objective data available to Defendant Clearview regarding whose biometric identifiers and information it has obtained. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice. All members of the proposed Classes are readily ascertainable because Defendant Clearview has access to information regarding the identity of each person whose biometric identifier and information it has obtained.

53. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the proposed Class. Common questions include, but are not limited to the following:

- a. Whether Defendant Clearview engaged in wrongful conduct as alleged herein;
- b. Whether Defendant Clearview has acted under color of law;

- c. Whether Defendant has violated the First Amendment of the United States Constitution;
- d. Whether Defendant Clearview has violated the Fourth and/or Fourteenth Amendments of the United States Constitution;
- e. Whether Defendant Clearview has violated the Contracts Clause of Article I of the United States Constitution;
- f. Whether Defendant Clearview provided Plaintiff and Class Members with the written information required by BIPA;
- g. Whether Defendant Clearview obtained written releases from Plaintiff and Class Members as required by BIPA;
- h. Whether Defendant Clearview had in place – and disclosed to the public – the written policies required by BIPA;
- i. Whether Plaintiff and Class Members suffered damages as a proximate result of Defendant Clearview; and
- j. Whether Plaintiff and Class Members are entitled to damages, equitable relief and other relief.

Moreover, based on Defendant Clearview's public statements, there is no reason to believe it treated any of the images on which it performed a facial geometry scan differently from any others in terms of obtaining the images, the information collected, the disclosures provided or not provided, the consent obtained or not obtained, the dissemination of the biometric scans to third parties, or the existence or nonexistence of a retention and destruction schedule. In short, whether Clearview violated BIPA's requirements is a question that can uniformly be answered for all Class Members, including Plaintiff.

54. **Typicality.** Plaintiff's claims are typical of the claims of the Classes he seeks to represent because Plaintiff and all members of the proposed Classes have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests to advance adverse to the interests of the other members of the proposed Class.

55. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed Class and has retained as his counsel attorneys experienced in class actions and complex litigation.

56. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of single adjudication, economy of scale and comprehensive supervision by a single court.

57. In the alternative, the proposed classes may be certified because:

- a. The prosecution of separate actions by each individual member of the proposed Classes would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendant Clearview;
- b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class

Members or which would substantially impair their ability to protect their interests; and

c. Defendant Clearview acted or refused to act on grounds generally applicable to the proposed classes, thereby making final and injunctive relief appropriate with respect to members of the proposed Class.

58. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification – namely the issues described in paragraph 53, above, because resolution of such issues would advance the disposition of the matter and the parties' interests therein.

CLAIMS FOR RELIEF

COUNT ONE **(VIOLATION OF FIRST AMENDMENT – DENIAL OF ACCESS TO COURTS)** **(On behalf of the Constitutional Rights Class)**

59. Plaintiff restates and realleges all paragraphs of this Complaint, as though fully set forth herein.

60. Defendants knowingly and illicitly interfered in Plaintiff's and Class Members' contracts with the platforms and websites to which they entrusted their photographs. In violation of the terms of use of those sites, Defendants used automated methods to obtain billions of photographs through "scraping" and other similar techniques which the websites prohibited.

61. Knowing that these forgoing processes would violate the terms of use and/or other actionable rights, Defendants proceeded to engage in that conduct understanding that doing so would impair and violate Plaintiff's and Class Members' rights.

62. Defendants could have easily afforded prior notice to the Plaintiff and Class Members and a process to object to and challenge the anticipated conduct. Defendants

knowingly failed to do so, likely because doing so would have resulted in judicial orders preventing Defendants from engaging in the very conduct.

63. Defendants engaged in this conduct in conspiracy with state officials so that (a) the scheme coming to light until after it was too late for Plaintiff and Class Members to seek judicial relief to prevent the scraping, collection and extraction of the biometric information; and (b) the information would not come to light through whistleblowers and other mechanisms for transparency of state action. All of the foregoing contributed to the inability to seek a judicial order enforcing Plaintiff's and Class Members' rights to prohibit the gathering of the data.

64. Plaintiff and Class Members demand judgement against Defendants Clearview, Ton-That and Schwartz, jointly and severally, in an amount to be determined together with their reasonable fees and costs in pursuing this action.

COUNT TWO
(VIOLATION OF THE FOURTH AMENDMENT)
(On behalf of the Constitutional Rights Class)

65. Plaintiff restates and realleges all paragraphs of this Complaint, as though fully set forth herein.

66. By all of the above, Defendants, acting under color of law, have engaged in unreasonable search and unreasonable seizure. Using techniques proscribed by the terms of service of various platforms and websites, specific statutory directives, and, in general contractual rights, Defendants obtained data entrusted to those platforms and websites without seeking permission or authorization. There was no warrant, no probable cause, no suspicion whatsoever to justify the collection of this information regarding Plaintiff and Class Members.

67. Defendants, acting under color of law and in conspiracy with state officials, extracted Plaintiff's and Class Members' biometric identifiers and information and made them

searchable, and in so doing enabled state-directed searches that violated Plaintiff's and Class Members' reasonable expectation of privacy. Defendants enabled biometric searches that could link Plaintiff's and Class Members' images to photographs they had posted, photographs others had posted of them, and photographs of them they did not even know existed. Plaintiff and Class Members had a reasonable expectation that these techniques would not be used (by state actors, their co-conspirators, their agents or others) to cobble together a database to automatically and instantaneously identify them from these photos.

68. Defendants went out of their way to keep their activities under the radar precisely so that affected individuals would not know or expect that their images were being collected or used in this way. This pattern of behavior further highlights the obvious fact that Plaintiff and Class Members could not reasonably expect to have all of their images vacuumed up indiscriminately by Defendants and made available for unlimited searches regardless of suspicion.

69. The searches and seizures are also rendered unreasonable, independent of the illicit method of gathering the information, due to the purpose for which they were undertaken – namely, the assembly, maintenance, and updating of a massive database intended to allow the biometric searching and tracking of tens or hundreds of millions of American citizens without the slightest grounds to suspect them of any misdeed.

70. Plaintiff and Class Members demand judgement against Defendants Clearview, Ton-That and Schwartz, jointly and severally, in an amount to be determined together with their reasonable fees and costs in pursuing this action.

COUNT THREE
(VIOLATION OF THE FOURTEENTH AMENDMENT)
(On behalf of the Constitutional Rights Class)

71. Plaintiff restates and realleges all paragraphs of this Complaint, as though fully set forth herein

72. Defendants, acting individually and in conspiracy with state officials, interfered in Plaintiff's and Class Members' rights in multiple ways which separately and cumulatively violate the Fourteenth Amendment Due Process Clause. Among these are the following:

- a. Defendants knowingly and illicitly interfered in Plaintiff's and Class Members' contracts with the platforms and websites to which they entrusted their photographs. In violation of the terms of use of those sites, Defendants used automated methods to obtain billions of photographs through "scraping" and other similar techniques which the platforms and websites prohibited when Plaintiff and Class Members uploaded these photos.
- b. Knowing that these forgoing processes would violate the terms of use, Defendants proceeded to engage in that conduct understanding that doing so would impair and violate Plaintiff's and Class Members' contractual rights. Defendants could have easily afforded prior notice to Plaintiff and Class Members and a process to object to and challenge the anticipated conduct. Defendants knowingly failed to do so, likely because doing so would have resulted in judicial orders preventing Defendants from engaging in the very conduct.

c. Defendants' conduct in conspiring to surveil millions of Americans and in violating their contractual rights threatens fundamental concepts of ordered liberty, risks interfering in and dissuading the exercise of numerous incidents of citizenship, including rights of public assembly, and puts them in jeopardy of future injury as by hacking, identity theft, stalking by domestic violence assailants, and in multiple other ways.

73. These harms are ongoing. As long as Defendant Clearview continues building, maintaining, and providing access to its database of images organized and searchable by biometric identifiers, American citizens face dramatically heightened surveillance risks any time they exercise the constitutionally protected rights of public assembly, political speech, and travel. Only the disabling and deletion of Clearview's database will allow the Constitutional Rights Class to be able to fully exercise these and other protected rights.

74. Plaintiff and Class Members demand judgement against Defendants Clearview, Ton-That and Schwartz, jointly and severally, in an amount to be determined together with their reasonable fees and costs in pursuing this action.

COUNT FOUR
(VIOLATION OF CONTRACTS CLAUSE – ART. I, U.S. CONSTITUTION)
(On behalf of the Constitutional Rights Class)

75. Plaintiff restates and realleges all paragraphs of this Complaint as though fully set forth herein.

76. By all of the above, Defendants conspired with municipalities that acted through ordinance and contract to further their illegal scheme as alleged herein.

77. As a direct result, Plaintiff's and the Class Members' rights not to have their data scraped in violation of the terms of use was and will continue to be impaired.

78. Plaintiff and Class Members demand judgement against Defendants Clearview, Ton-That and Schwartz, jointly and severally, in an amount to be determined together with their reasonable fees and costs in pursuing this action.

COUNT FIVE
(EXPUNGEMENT)
(On behalf of all Classes)

79. Plaintiff restates and realleges all paragraphs of this Complaint, as though fully set forth herein.

80. By all of the above, Defendants have assembled a private database to use, *inter alia*, as a set of records for investigation of potential criminality by persons who have committed no offense and who must be presumed innocent.

81. As explained above, the potential adverse consequences to Plaintiff and Class Members in the database are paramount and completely outweigh any legitimate interest in the keeping of such records. Moreover, the database was assembled in violation of contractual and other rights of Plaintiff and Class Members.

82. In the manner explained above, and otherwise, the maintenance and dissemination of these records impact and have the potential to bring about a violation of both federal constitutional and state law rights.

83. Plaintiff and Class Members demand judgement against Defendants Clearview, Ton-That and Schwartz, jointly and severally, requiring expungement of all records and data regarding the Class Members.

COUNT SIX
(VIOLATION OF BIPA – 740 ILCS § 14/15(c))
(On behalf of the Illinois Class)

84. Plaintiff restates and realleges all paragraphs of this Complaint, as though fully set forth herein.

85. As alleged above, Defendants violated BIPA by unlawfully selling, leasing, trading and otherwise profiting from an individual's biometric identifier or biometric information, including the biometric identifiers and information of Plaintiff and Class Members.

86. Defendants' violation of BIPA was intentional or reckless or, pleaded in the alternative, negligent.

87. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages.

88. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

89. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

90. Plaintiff and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT SEVEN
(VIOLATION OF BIPA – 740 ILCS § 14/15(d))
(On behalf of the Illinois Class)

91. Plaintiff restates and realleges all paragraphs of this complaint as though fully set forth herein.

92. As alleged above, Defendants violated BIPA by disclosing, redisclosing and otherwise disseminating individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Members, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure or redisclosure; (b) the disclosure or redisclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure or redisclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

93. Defendants' violation of BIPA was intentional or reckless or, pleaded in the alternative, negligent.

94. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages.

95. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

96. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by

unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

97. Plaintiff and Class Members also seek punitive damages, injunctive relief and the reasonable attorneys' fees, costs and expenses relating to this action.

COUNT EIGHT
(VIOLATION OF BIPA – 740 ILCS § 14/15(b))
(On behalf of the Illinois Class)

98. Plaintiff restates and realleges all paragraphs of the Complaint as though fully set forth herein.

99. As alleged above, Defendants violated BIPA by failing to develop a written policy that it made available to the public that established a retention schedule and guidelines for permanently destroying biometric identifiers and information.

100. Defendants' violation of BIPA was intentional or reckless or, pleaded in the alternative, negligent.

101. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages.

102. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

103. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the

injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

104. Plaintiff and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT NINE
(VIOLATION OF BIPA – 740 ILCS § 14/15(a))
(On behalf of the Illinois Class)

105. Plaintiff restates and realleges all paragraphs of this Complaint as though fully set forth herein.

106. As alleged above, Defendants violated BIPA by collecting or otherwise obtaining individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiff and Class Members, without providing the requisite written information and without obtaining the requisite written release.

107. Defendants' violation of BIPA was intentional or reckless or, pleaded in the alternative, negligent.

108. As a direct and proximate result of Defendants' violations of BIPA, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages.

109. Plaintiff and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

110. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the

injuries in that a judgment for monetary damages will not end the misuse of Plaintiff's and Class Members' biometric identifiers and information.

111. Plaintiff and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT TEN
(UNJUST ENRICHMENT)
(On behalf of all Classes)

112. Plaintiff restates and realleges all paragraphs of this Complaint as though fully set forth herein.

113. Defendants obtained a monetary benefit from Plaintiff and Class Members to their detriment. Defendants did so by profiting off of the covert collection of the biometric identifiers and information of Plaintiff and Class Members, while exposing Plaintiff and Class Members to radically heightened risk of surveillance both now and in the future.

114. Plaintiff and Class Members did not authorize Defendants to collect, disclose, redisclose, sell, lease, trade or otherwise profit off their biometric identifiers and information.

115. Defendants appreciated, accepted and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiff and Class Members as described herein.

116. Defendants sold, leased, traded and otherwise profited from – and caused to be sold, leased, traded and otherwise profited from – Plaintiff's and Class Members' biometric identifiers and information and did not provide full compensation for the benefit received from Plaintiff and Class Members.

117. Defendants acquired and caused to be acquired Plaintiff's and Class Members' biometric identifiers and information through inequitable means in that they covertly scraped

Plaintiff's and Class Member's online photos and corresponding information without permission and in violation of Illinois law.

118. Plaintiff and Class Members have no adequate remedy at law.

119. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits obtained from Plaintiff and Class Members.

120. Under the principles of equity and good conscience, Defendants should not be permitted to retain the biometric identifiers and information belonging to Plaintiff and Class Members because Defendants unlawfully obtained that information.

121. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from the sale, lease and/or trade of Plaintiff's and Class Members' personal information.

COUNT ELEVEN
INJUNCTIVE RELIEF
(On behalf of all Classes)

122. Plaintiff restates and realleges all paragraphs of this Complaint as though fully set forth herein.

123. Plaintiff and Class Members have clear and ascertainable rights in need of protection – namely: (a) the rights under the U.S. Constitution alleged herein; (b) the right to have Defendants abide by their obligations under BIPA; and (c) the right to control their biometric identifiers and information; and (d) the right to privacy.

124. Plaintiff and Class Members have no adequate remedy at law because a legal remedy cannot retrieve the biometric identifiers and information that Defendants unlawfully collected, sold, leased, traded and otherwise profited from and cannot end the invasion of privacy caused by Defendants' conduct.

125. Plaintiff and Class Members will suffer irreparable harm, as alleged herein, from Defendants if their conduct is not so restrained, requiring injunctive relief.

126. Plaintiff and Class Members are likely to succeed on the merits because, as alleged herein, Defendants unlawfully collected, sold, leased, traded and otherwise profited from Plaintiff's and Class Member's biometric identifiers and information despite being prohibited from doing so.

127. Plaintiff and Class Members seek injunctive relief: (a) barring Defendants from any further use of Plaintiff's and Class Members' biometric identifiers and information; (b) barring Defendants from continuing to collect, capture or otherwise obtain Plaintiff's and Class Member's biometric identifiers and information; and (c) requiring Defendants to delete and destroy Plaintiff's and Class Members' biometric identifiers and information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff David Mutnick, on behalf of himself and on behalf of the Classes, respectfully seeks from the Court the following relief:

- a. Certification of the Classes as requested herein;
- b. Appointment of Plaintiff as Class representative and his undersigned counsel as Class counsel;
- c. Award Plaintiff and members of the proposed Classes damages, including statutory and punitive damages;
- d. Award Plaintiff and the proposed Classes an order requiring expungement of records;
- e. Award Plaintiff and members of the proposed Classes equitable, injunctive and declaratory relief, including the enjoining of Defendant Clearview from

any further use of individuals' biometric identifiers and information; from continuing its unlawful business practices, as alleged herein; and requiring the deletion and destruction of all biometric identifiers and information in its possession, custody and control;

- f. Award Plaintiff and members of the proposed Classes pre-judgment and post-judgment interest as permitted by law;
- g. Award Plaintiff and members of the proposed Classes reasonable attorneys' fees and costs of suit, including expert witness fees; and
- h. Award Plaintiffs and members of the proposed Classes any further relief the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: January 22, 2020

Respectfully submitted,

/s/ Scott R. Drury
SCOTT R. DRURY

Arthur Loevy
Michael Kanovitz
Jon Loevy
Scott R. Drury
LOEVTY & LOEVTY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
arthur@loevy.com
mike@loevy.com
jon@loevy.com
drury@loevy.com